REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-06-2010	FINAL	

4. TITLE AND SUBTITLE

Coping with Uncertainty: Command and Control in Information Degraded Environments

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LT Michael W. Kessler, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department

Naval War College

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Coping with Uncertainty: Command and Control in Information Degraded Environments. The contemporary operational level commander is accustomed to leveraging an abundance of information within a highly collaborative headquarters, with a centralized command and staff structure at his disposal. The era of "forward reach" has provided persistent connectivity at all levels of war, which commanders have used to their advantage in on-going conflicts. As technology and human decision-making are inextricably linked through Command and Control (C2), a future operating environment where networks and information are degraded begets sobering implications for the Joint Force Commander. This study explores C2 theory in context with the future operational environment – specifically, information domain threats to U.S. C2. Conclusions and recommendations concerning doctrine, training, education, and command organization pertain to challenges and opportunities in future C2 constructs, with an emphasis on humanistic approaches to C2.

15. SUBJECT TERMS

Command and Control, C2, Network Centric Warfare, Information Operations, Hybrid Warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Department
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		**26**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3414

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Coping with Uncertainty: Command and Control in Information Degraded Environments

by

Michael W. Kessler

Lieutenant, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ___/original signed/____

03 May 2010

Contents

Abstract

Coping with Uncertainty: Command and Control in Information Degraded Environments. The contemporary operational level commander is accustomed to leveraging an abundance of information within a highly collaborative headquarters, with a centralized command and staff structure at his disposal. The era of "forward reach" has provided persistent connectivity at all levels of war, which commanders have used to their advantage in on-going conflicts. As technology and human decision-making are inextricably linked through Command and Control (C2), a future operating environment where networks and information are degraded begets sobering implications for the Joint Force Commander. This study explores C2 theory in context with the future operational environment – specifically, information domain threats to U.S. C2. Conclusions and recommendations concerning doctrine, training, education, and command organization pertain to challenges and opportunities in future C2 constructs, with an emphasis on humanistic approaches to C2.

Introduction

Today's operational level commander is accustomed to leveraging an abundance of information within a highly collaborative headquarters, with a centralized command and staff structure at his disposal. The era of "forward reach" has provided persistent connectivity at all levels of war, which commanders have used to their advantage in Iraq and Afghanistan.[1] As technology and human decision-making are inextricably linked through C2, a future operating environment characterized by hybrid threats where networks and information may be degraded begets sobering implications for the Joint Force Commander.[2] To ensure success in an information degraded environment, the Joint Force needs to adapt doctrine, training and education, and command organization to enable a C2 process capable of coping with uncertainty. Commanders and subordinates at every level must be able to "act without instructions per Commander's intent."[3]

In order to derive conclusions pertinent to the Joint Force, this study will start by defining relevant terms and bounding the scope of the discussion. Theories will then be explored to contextualize contemporary C2, and it will be proved that the future operating environment will likely be riddled with information domain challenges pertaining to C2. By juxtaposing the future operating environment with current operations, the theory will be applied to develop recommendations pertaining to doctrine, training, education, and command organization which provide the Joint Force with the flexibility to operate effectively in information degraded environments.

C2 Defined

An hour of research through scholarly bodies of materials will leave the reader with a myriad of definitions pertaining to Command and Control. Literature from

electronics manuals to scholarly works on philosophy and leadership all contain definitions pertaining to C2.[4] Because of the duality inherent in C2 constituting the humanistic and the technological; the art and the science; the process and the system, many of these definitions – whether pertaining to a thermostat for an air conditioner or a treatise on motivational leadership – bear relevant notions for military practitioners to use in their personal thinking on C2. However, definitions from Joint Doctrine are most appropriate within the scope of this study.

From *Joint Operations* (JP 3-0), Command and Control is defined as "the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission."[5] Defined individually in JP 3-0, Command "includes the authority and responsibility for effectively using available resources to accomplish assigned missions,"[6] while Control is "inherent in command to regulate forces and functions and execute commander's intent."[7]

JP 3-0 discusses the dual nature of command, citing that "command at all levels is the art of motivating *and* directing people and organizations into action to accomplish missions."[8] [emphasis added] This is often referred to as the difference between leadership and management. In discussing C2, it is not practical to decouple motivating from directing, or leadership from management. However, pertinent to this study, discussions of C2 will focus on the process that supports the commander's decision-making. That is, "the down to earth questions: who ordered whom to do what, when, by what means, on the basis of what information, what for, and to what effect."[9]

C2 Theory

In order to postulate how the Joint Force ought to maintain effective C2 in an information challenged environment, it is helpful to draw on theory that is tailored to military decision-making processes in order to establish a framework upon which the C2 process can be matched to the conditions at hand. Relevant theories which vary greatly are captured in Dr. Martin van Creveld's *Command in War,* and the theory surrounding Network Centric Warfare (NCW), postulated by Drs. David S. Alberts and Richard E. Hayes in *Understanding Command and Control*.

In *Command in War*, Martin van Creveld evaluates the history of C2 from the "Stone Age of Command" prior to 1800, to the Vietnam War. *Command in War* was published in 1985, at the dawn of the information age. Van Creveld's theory is historically grounded, and frames C2 on what he calls commander's "quest for certainty."[10] Acknowledging the interrelationship between the decision making process and technology inherent in C2, Van Creveld's theory governs C2 in a way that transcends communications and technological developments.

Certainty, according to van Creveld, is the product of two factors: the amount of information available and the nature of the task at hand. Throughout history, the evolution of C2 can be described as "a race between the demand for information and the ability of command systems to meet it."[11] What follows then could be an argument that with unlimited bandwidth comes infinite information, and an approach to absolute certainty—and therefore, ideal C2. Van Creveld refutes the possibility for absolute certainty in war through historical analysis which shows that armies become no better at handling increased information over time relative to the task at hand. The insufficiency

of information has persisted over time, he says. Information is often "not available on time," "superabundant," or simply "wrong."[12]

According to van Creveld, the concept of absolute certainty is a fallacy. Furthermore, the information networks of the future will produce no more certainty than present systems, due to the nature of war. War is interactive, and the maxim that the enemy gets a vote holds true in matters of the commander's certainty. War elicits the passions of the people involved. "Fear, anger, vindictiveness, and hatred"[13] persuade the commander making decisions, his staff processing information, and, most importantly, the enemy. Because each side acts in self-interest and is free to impose himself on the other, "the attainment of certainty is, a priori, impossible."[14]

Certainty, as a product of the amount of information available and the nature of the task, provides the framework around which van Creveld suggests that commanders design C2 arrangements. If one of the factors is held constant, an inverse relationship can be derived between the other factor and certainty. In keeping the amount of information available constant, certainty varies with the nature of the task. If the scope of the task at hand is expanded, then certainty goes down, and so too does the efficiency of the organization vis-à-vis the objective. Likewise, for a given task, certainty goes up with more information, and down with less information—and efficiency follows.

Using the relationship between information available, the nature of the task and certainty, van Creveld says,

> Confronted with a task, and having less information than is needed to perform that task, an organization may react in either of two ways. One is to increase its information—processing capacity, the other to design the organization, and indeed the task itself, in such a way as to enable it to operate on the basis of less information. These approaches are exhaustive;

> no others are conceivable. A failure to adopt one or the other will automatically result in a drop in the level of performance.[15]

It is around this choice that the fundamental issue of C2 hinges: whether to cope with uncertainty by designing C2 arrangements for it, or to seek certainty in information gathering and processing. Van Creveld, drawing on his historical analysis, categorically states that militaries who cope with uncertainty will experience better outcomes in war.

As part of his conclusions, van Creveld poses five interrelating dictums for C2 arrangements designed to cope with uncertainty. First, decision thresholds should be set at a low-level in the chain of command. Second, self-contained units should exist at a level corresponding to the decision thresholds. Third, information sharing should be facilitated through regular reporting and transmission up and down the chain of command. Fourth, headquarters elements should implement means to pull information from whatever level it pleases to supplement regular reports. Fifth, and finally, the organization must maintain avenues for formal and informal communications.[16]

An alternative to van Creveld's theory can be found in the bodies of literature surrounding Network Centric Warfare (NCW). In general terms, NCW is a concept that seeks, through network enablers, a shared awareness in every domain. At some point in the building of shared awareness, a tipping point will occur, facilitating self-synchronization within the organization. Consequently, an abundance of agility and effectiveness will ensue.[17]

In many cases, NCW has increased efficiency at the operational level of war. In the on-going conflicts in Iraq and Afghanistan, for example, NCW has enabled the Joint Force Air Component Commander (JFACC), for example, to reach unprecedented levels of efficiency by using reachback, collaboration, and a tailored command structure—all

enabled by NCW principles and architecture manifested in the Air Operations Center (AOC).[18] Operating as a theater component in U.S. Central Command (CENTCOM), the JFACC has been able to apply centralized air assets to support ground operations characterized by decentralization and "localized strategy to task" over two theaters of war simultaneously.[19] Clearly, by successfully managing low density/high demand assets across the dichotomy of centralized airpower and decentralized ground operations, the JFACC has proved the utility of NCW principles.

However, the body of literature concerning NCW admits its insolvency in the absence of a robust information network. According to Alberts and Hayes, networks are social in nature, and based upon patterns of interaction; it is the fidelity of these interactions – and consequently the networks which underwrite such interactions – that determines the effectiveness of C2. The parameters that govern the fidelity of interactions include: extent, access, communications (bandwidth), level of participation, frequency, synchronicity, richness, and scope.[20]

An information degraded environment would be a forced departure from the maxims of the parameters of interaction; most likely, a departure from each parameter's maxim. As the operational environment forces the C2 process to slide down the spectrum of interaction fidelity, network collaboration would decrease until it unravels. Alberts and Hayes state that "such minimum collaboration would be unlikely to generate results different from those generated by an individual working alone."[21]

Presumably, before it falls apart, as information is degraded, the application of forces in pursuit of an objective would reach a tipping point where the C2 process—and hence the Commander—is no longer effective because the risk (to mission or force)

associated with decreased effectiveness has passed an acceptable level. NCW holds mission accomplishment hostage to information assurance without alternatives. Consequently, the U.S. military should seek to adapt C2 around a theory that provides an alternative to the Commander: the ability to cope with uncertainty. In considering a future operating environment where such an alternative is necessary, it is useful to examine the character of such an environment in the context with contemporary U.S. C2 in order to apply principles derived from C2 theory.

U.S. C2 in Context with the Future Operating Environment

Concurrent to its expansion of power after World War II, which included a robust network of overseas bases and power projection capability, U.S. dominance in the information domain ensued.[22] The United States' ability to gather, generate, and disseminate information across networks to aid in decision-making expanded far beyond any adversary's capability. As network technology evolved, it absorbed the intelligence and C2 functions into today's concept of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance). An example of the complexity in contemporary use of network enabled concepts can be found in the Navy's Forcenet concept, which is the Navy's "operational construct and architectural framework for naval warfare in the information age, which integrates warriors, sensors, networks … and weapons into a networked, distributed combat force."[23]

Information superiority, robust forward bases, and naval power are enablers for effective power projection and access generation that the U.S. has leveraged for decades. However, eight years after the U.S. projected power hundreds of miles into landlocked Afghanistan to defeat the Taliban in a matter of weeks, the U.S. is realizing a future

where unfettered access can no longer be assumed as a result of anti-access/area-denial (A2/AD) strategies being pursued by nations such as China and Iran.[24]

Burgeoning A2/AD capabilities, including short and medium range conventional ballistic missiles will likely hold U.S. bases at risk in the event of conflict, creating a double-edged sword: a cloak of American protection on one hand, and political and security liability on the other.[25] Furthermore, reports show China is developing the DF-21D anti-ship ballistic missile (ASBM), which could potentially threaten U.S. carriers—the icon of American forward presence—out to 1600 nm, thereby marginalizing, or possibly even rendering obsolete, U.S. naval presence inside the first island chain and beyond.[26] In addition to capabilities that threaten U.S. forward bases and naval presence, information warfare capabilities are proliferating that will extend its A2/AD measures beyond the sea, air and land domains into space and cyber space—thereby threatening U.S. information superiority.

Although intentions remain unclear, China looks to be developing capabilities to contest adversaries' use of space-based services, including communications, imagery, and navigation. China is developing satellite denial capabilities across the spectrum from jamming and blinding to non-kinetic mission-kill using "high-powered lasers, particle beams, and electro-magnetic pulse devices."[27] Furthermore, China is also developing kinetic kill capability using anti-satellite (ASAT) weapons, which when tested successfully in 2007, confirmed a kinetic kill capability several years in advance of U.S. intelligence estimates.[28]

While the specifics of Chinese cyberspace capabilities remain cloaked in a shroud of secrecy, they are believed to be an emerging threat to U.S. military operations.[29] The

2009 DoD Annual Report to Congress on the Military Power of the People's Republic of China documents this growing cyber capability. Networks around the world have been the subject of attacks that appear to originate in China, though it is unconfirmed whether the attacks were sanctioned by the Chinese government or People's Liberation Army (PLA). While these attacks are mostly intrusions that exfiltrate data, the requisite skills associated with them are said to translate well into military applications of computer network attack (CNA). Furthermore, Chinese writings allude to the desire to find an "assassin's mace" capability in the information domain.[30]

In describing the A2/AD threat, it is important to take a holistic, inclusive view of the threats around the world, so as to avoid thinking that A2/AD threats in the information domain are limited to conventional near-peer competitors—like China—who some might say the United States is unlikely to face in military conflict. Evidence of the proliferation of A2/AD capabilities can be found in the *INS Hanit* incident, where an Israeli corvette was struck by land-based cruise missile in the summer of 2006, killing four Israeli sailors, and causing significant damage to the ship.[31] The Lebanese insurgent group, Hezbollah reportedly obtained the C-802, a Chinese produced low-end, land based version of the Exocet anti-ship cruise missile (ASCM), from Iran. The C-802 crew managed to operate the missile not with a high-tech fire control radar system, but by tying it in to the Lebanese coastal defense radar.[32]

Hezbollah's employment of the C-802 brings front and center a salient issue for U.S. defense planners: future A2/AD capabilities will transcend into the realm of hybrid warfare. An example relevant to the information domain—and therefore, to C2—is shown from recent accounts of non-state sanctioned cyber capabilities. In a report

entitled *Shadows in the Cloud: Investigating Cyber Espionage 2*.0, Canadian cyber security firms revealed the interface between crime and espionage in the cyber domain.[33] Just as the mission assurance of the *INS Hanit*, a conventional warfighting platform, was compromised by a hybrid threat, the evidence presented suggests that U.S. networks may be vulnerable to attack from non-state actors as well. In turn, the responsibility for adapting C2 to the A2/AD environment transcends any one geographic or specified combatant command, or any one service.

Given the circumstantial evidence regarding the character of A2/AD threats writ large, and the discrete, emerging threats in the information domain, C2 under A2/AD conditions in the information domain will likely take the form of degraded networks – fractional bandwidth, compromised common operational pictures, locally jammed communications and sensors, etc. However, one cannot rule out a near total loss of modern communications. While deterministic approaches should be avoided, clearly, the future Joint Force commander will exercise C2 in pursuit of objectives under a range of conditions from the current state of the art to "the stone age of command."[34]

In considering future warfare, Van Creveld's theory provides a useful point of departure for conceptualizing C2 in information degraded environments, because it implies that when faced with a failure of communications systems, the commander, instead of thinking about how to overcome the new information deficit, might realize he never needed that information. Alternatives to be exploited exist and can be constructed according to his general principles for effective C2: low-level decision thresholds and corresponding self-contained units; push and pull of information up and down the chain of command; and both formal and informal methods of communication. Admittedly, this

line of thinking – the decision to cope with uncertainty – beseeches an organizational cultural change of magnificent proportions for the Joint Force at the operational level, which has been operating both efficiently and effectively in on-going conflicts by centralizing high-demand low-density resources, sharing massive amounts of information, and relying on support relationships, which permits retention of control of organizations at a high level in the chain of command.[35]

Exformation: Abating the Information Deficit

Several recent initiatives by U.S. Joint Forces Command (JFCOM) indicate a conscious effort to guide the Joint Force in once again coping with uncertainty. In his *Vision for a Joint Approach to Operational Design*, General Mattis says, "our goal is to develop a joint force that acts in uncertainty and thrives in chaos through a common understanding of the essence and nature of the problem and the purpose of the operation."[36] Thriving is a maxim that exceeds coping, but may represent a mandate imposed by the future operational environment. In order to do either, the Joint Force must take steps to mitigate the information deficit imposed by the enemy and the environment.

To challenge the conventional wisdom: an information deficit actually does not create a void of hopelessness that the Joint Force can only fill with monumental risk less it be precluded from achieving its objective. Rather, an information deficit provides the opportunity to harness what the Danish physicist Tor Norretranders calls "exformation."[37] Put simply, exformation is information that is *explicitly* discarded—not discarded on accident, or because the originator forgot about it. According to

Norretranders, the shared body of knowledge between entities contains far greater meaning than what can be communicated directly in the form of information.[38]

The story of Admiral Nelson's signaling at the Battle of Trafalgar provides a succinct notion of the power of exformation in the context of a C2 process designed at coping with uncertainty. As *HMS Victory* led the Royal Navy on approach to the enemy in October 1805, Nelson, armed with a new signal manual that had never been used by a fleet in combat, sent one last message to his subordinate commanding officers before the engagement: "England expects that every man will do his duty."[39]

Prior to Trafalgar, Nelson and his subordinates became known as the "Band of Brothers,"[40] a term derived from Shakespeare's Henry V, and reflective of the trust and affection reciprocated between Nelson and his men. The exformation contained in Nelson's signal was what he specifically did *not* say: the connotations of a shared body of knowledge developed over years of war council meetings, mind melding, and training.[41] By intentionally leaving out what he trusted his subordinates to know, Nelson's message was impregnated with profundity beyond the depths of signal flags—or video teleconferencing, for that matter.

Recommendations and Conclusions:

In terms of emerging doctrine, JFCOM is taking steps through its *Vision for a Joint Approach to Operational Design* to provide the Joint Force with a framework to realize the power of exformation and cope with uncertainty in information mitigated environments. Operational design, as defined in JP 3-0, is "the conception and construction of the framework that underpins a campaign or major operation plan and its subsequent execution."[42] Emphasizing Design will impel the Joint Force to "think deeply

about the fundamental nature of a complex military problem,"[43] which will pay dividends when commanders and their subordinates share an understanding of the operational environment, allowing exformation—vice information—to underwrite C2.

The professional military education system is a critical enabler for the Joint Force to affect a degree of transition away from a heavy reliance on information. Operating without instructions, per Commander's Intent, requires a shared body of knowledge relevant to the task at hand. Emphatically promoting the need for professional military education, Dr. Colin S. Gray points out that flag or general officers at the operational level, unable to sequester themselves in a political vacuum, are charged with formulating and translating prudent strategy into tactics (and vice versa) at a nexus permeated by politics and policy.[44] Education can contribute to an individual's development of relevant knowledge necessary to thrive in complex, interactive environments like the operational level of war.

Education that applies critical thinking to theories of C2 will produce officers who are able to design and apply an appropriate C2 structure rather than simply relying on exquisite technological solutions when confronted with an objective and an interactive enemy. Specifically, it is not enough to understand what constitutes centralization or decentralization, the advantages or disadvantages of either, or to draw a historical C2 diagram from the last great campaign, or on-going operations. Rather, officers at the operational level must be able to conceive innovative ways to manage varying degrees of information assurance across the range of military operations while sustaining effectiveness.

Concerning practical experience and the aggregation of personal experience relating to C2, training is a necessary complement to the education piece. Ultimately, information degraded C2 operations should be incorporated into major joint exercises, like it was in the June 2009 Capstone Concept for Joint Operations (CCJO) Experiment war game.[45] While one can imagine the useful insights and lessons learned from such a game, these principles also should be part of on-going training for the serving operational commanders and staffs, as well as joint task force, and component level headquarters certifications.

Admittedly, some training benefit—as well as time and resources—might be lost if a major fleet, corps, or operational level exercise is devoured by a C2 "booby trap." However, lesser training evolutions can be executed, still at the operational level, such as staff drills and war games that will facilitate a ramp up to major exercises incorporating tactical units—necessary to provide the commander and his staff with experience germane to C2 in information degraded environments.[46] For example, the GameNet system residing in the War Gaming Department at the U.S. Naval War College in Newport, RI has embedded characteristics that can train players to such an environment. Using GameNet, the control cell can throttle bandwidth to each cell, simulate network loads for the staffs to manage, and utilize quality of service monitors.[47] All of these features can teach staffs how to "fight the network,"[48]—i.e., sustain the C2 process as the enemy systematically targets the network.

Provided that doctrine, education, and training can be oriented towards coping with uncertainty, decentralization would be practicable. Returning to van Creveld's stated relationship between certainty, information processing, and the task at hand: the

commander pursuing an objective in an information deficit can decentralize, thereby permitting his or her organization to operate with less information. The Joint Force must be constituted of self-contained units at the appropriate low level in order to make such decentralization possible.[49]

The Joint Task Force (JTF) and corresponding component commander constructs provide the necessary flexibility in command organization because they are usually established at the outset of a crisis, and therefore, are tailored to the objective. The JTF and its components have a certain degree of de facto freedom from service administration and logistics, but it must be understood that they are often formed out of service component commands or subordinates.[50] So, for the Joint Force at-large, and the service components, consideration must be given to organizing for decentralization.

An implication of decentralization is the need to think differently about battlespace geometry and the assignment of commanders. In the practical context of contemporary operations, it is likely that information degraded environments will preclude the theater level consolidation of high-demand/low-density assets—à la "the [current] CENTCOM model."[51] Of note, the Navy and the Joint Force Maritime Component Commander (JFMCC) are headed in a similar direction as the JFACC with the development of the Maritime Operations Center (MOC) Concept, a networked C2 infrastructure. Both the MOC and the AOC dictate alignments of doctrine, organization, training, education, and personnel towards the polestar of networked, centralized C2 on the theater-component level.[52]

When choosing a command to take on the responsibilities of a JFMCC or JFACC, if, for example, only line-of-sight communications were available in the area of

operations, it would likely be necessary to unhinge that commander from his respective AOC or MOC. In this case, embarking a numbered fleet commander on a flag ship or deploying a numbered air force commander in order to position them appropriately so that they are relevant to the fight would need to be considered. Similar parameters exist at the JTF level, where it may be prudent for the commander to exercise his authority to establish one or more subordinate JTFs.[53]

In short, information degraded environments constrain the commander's span of control, thereby necessitating a division of tasks among subordinates, which creates decentralization. Commanders may find it necessary to divide assets into smaller geographical areas of operation vice task oriented commanders operating over an expanse of a theater functional domain. Consequently, each commander may experience greater autonomy, but in smaller operational area. Other situations might demand the same from other components, depending on the objective, the forces to be employed, the resources available, the acceptable level of risk, and, of course, interaction with the enemy.

Continued studies on this topic might include research, analysis, and war gaming pursuant to emerging doctrine with operational level C2 impacts, such as the Air Sea Battle Concept.[54] The adequacy of C2 themes throughout Joint Force training and professional military education should be reviewed to ensure commanders and subordinates are prepared to conceive C2 solutions that align ends, ways, and means. Finally, implications of decentralization should be thoroughly examined—specifically, the preparedness of lower level commanders to assume the responsibility held by contemporary senior commanders.

In conclusion, network enabled technologies, such as the MOC and the AOC represent tremendously powerful concepts that comply with JFCOM's Vision of C2 that is "leader-centric and network-enabled."[55] Not to take advantage of network-enabled C2 capabilities would be unforgivable. However, the future operating environment is unpredictable at worst; and at best, represents a conflation of state and non-state actors possessing a variety of capabilities that can target U.S. C2 networks. Consequently, the Joint Force must pursue humanistic development of C2 solutions just as fervently as it seeks technological eminence.

Notes

[1] Michael M. Phillips, "Civilians in the Crosshairs Slow Troops," *Wall Street Journal*¸ 22 February 2010, 1. Irregular warfare (IW) is defined as "a violent struggle among states and non-state actors for legitimacy and influence over the relevant populations. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities." U.S. Department of Defense, *Irregular Warfare Joint Operating Concept* (Washington, DC: U.S. Department of Defense, September 2007), 6.

[2] Mattis to U.S. Joint Forces Command, *C2 Vision*, memorandum. Hybrid warfare, often referred to as a convergence of types of belligerents and types of capabilities, is characterized by adversaries who "will most likely present unique combinational or hybrid threats specifically targeting U.S. vulnerabilities." Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly*, Issue 52 (1st Quarter 2009), 34-35.

[3] Ibid.

[4] Bjorkland, Raymond C., *The Dollars and Sense of Command and Control* (Washington, DC: National Defense University Press, 1995), 12-13.

[5] Chairmain, U.S. Joint Chiefs of Staff, *Joint Operations* final coordination with Ch1, 13 Feb 2008. Joint Publication (JP 3-0) (Washington, DC: CJCS, 17 December 2006), III-1

[6] Ibid., III-2.

[7] Ibid., III-5.

[8] Ibid., III-2.

[9] Van Creveld, Martin, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 12.

[10] Ibid., 264.

[11] Ibid., 265.

[12] Ibid.

[13] Ibid., 266.

[14] Ibid.

[15] Ibid., 269.

[16] Ibid., 270.

[17] Alberts, David S., and Hayes, Richard E., *Understanding Command and Control* (Washington, DC: CCRP Publication Series), 2. Networks, as they relate to C2 for the purpose of this study are defined as "the communications and data links that bring together the various elements of a military's intelligence, reconnaissance, surveillance (ISR) and targeting systems along with its command and control elements to provide prompt, precise guidance to munitions that can exploit it." Andrew Krepinevich, *Why AirSea Battle?* (Center for Strategic and Budgetary Assessments: Washington, DC, 2010), 6.

[18] William A. Woodcock, "The Joint Forces Air Command Problem: Is Network-Centric Warfare the Answer?," *Naval War College Review* (Winter 2003), 124-138.

[19] Gary Luck and Mike Findlay, *Joint Operations Insights & Best Practices, 2nd ed* (Suffolk, VA: Joint Warfighting Center, 2008), 44.

[20] Alberts and Hayes, *Understanding Command and Control*, 151-152.

[21] Ibid., 152.

[22] Krepinevich, *Why AirSea Battle?*, 5-7.

[23] Milan Vego, "Future Warfare at Sea: Decline of Decision-Making in Naval Operations?," *Naval Forces*, 1 January 2009, 10.

[24] Krepinevich, *Why AirSea Battle?*, vii.

[25] Ibid., 8-9.

[26] Erickson, Andrew S., and Yang, David G., "On the Verge of a Game Changer," *U.S. Naval Institute Proceedings*, May 2009, 26-32. The "first island chain" refers to the string of islands encompassing the East and South China Seas starting with Japan's main island to the north, and on down through the Ryukus, Senkakus, Formosa, Luzon, Palawan, Borneo, to the Malacca Straits.

[27] Mackey, James, "Recent US and Chinese Antisatellite Activity," *Air and Space Power Journal*, 1 October 2009, 84.

[28] Krepinevich, *Why AirSea Battle?*, 15.

[29] Ibid., 16.

[30] U.S. Department of Defense, *Annual Report to Congress: The Military Power of the People's Republic of China 2009* (Washington, DC: Office of the Secretary of Defense, 2009), 20. According to scholars from the China Maritime Studies Institute at the U.S. Naval War College, "assassin's mace," a widely used term in Chinese strategic literature, is best translated into English as "silver bullet." See Andrew S. Erickson, Lyle J.

Goldstein, and William S. Murray, "Chinese Mine Warfare: A PLA Navy 'Assassin's Mace' Capability," *China Maritime Studies*, no. 3 (Newport, RI: Naval War College, 2009), 59.

[31] Yaakov Katz Amir Mizroch, "Sailor Killed, Three Missing as Hizbullah Helped by Iran Fires Missile at Israeli Ship," *Jerusalem Post*, 16 July 2006, 1.

[32] Alon Ben-David and Richard Scott, "Intelligence failure led to strike on Hanit," *Janes Navy International*, 1 September 2006, http://search.janes.com (accessed 15 April 2010).

[33] Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Joint Report, http://shadows-in-the-cloud.net (accessed 10 April 2010), IV.

[34] Van Creveld describes the period before 1800 as "the Stone Age of Command," because of the characteristics of warfare - specifically the information available to the commander, his span of control, and the complexity of the forces he commanded. See Van Creveld, *Command in War*, 17-57.

[35] Luck and Findlay, *Insights and Best Practices*, 44. For details of Joint Force lessons learned and best practice pertaining to the operational level of war see Insights Papers available from the Joint Warfighting Center at http://www.jko.cmil.org.

[36] Mattis, James N., Commander U.S. Joint Forces Command to U.S. Joint Forces Command, *Vision for a Joint Approach to Operational Design*, memorandum, 6 October 2009.

[37] Norretranders, Tor, *The User Illusion: Cutting Consciousness Down to Size* (New York: Penguin, 1998), 92.

[38] Ibid., 92.

[39] Gordon, Andrew, *The Rules of the Game: Jutland and British Naval Command* (Annapolis, MD: Naval Institute Press, 2000), 159.

[40] Ibid., 158.

[41] Ibid.

[42] JP 3-0, *Joint Operations*, IV-3.

[43] Mattis to U.S. Joint Forces Command, *Operational Design*, memorandum.

[44] Colin S. Gray, *Schools for Strategy: Teaching Strategy for 21st Century Conflict* (Strategic Studies Institute: Carlisle, PA, 2009), 8-10.

[45] Daniel Wasserbly, "USJFCOM explores network-free warfighting," *Janes International Defence Digest*, 9 June 2009, http://search.janes.com (accessed 15 April 2010).

[46] Chairman, U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters,* Joint Publication (JP 3-33) (Washington, DC: CJCS, 16 February 2007), VII-6.

[47] Robert R. Rubel (Dean, Center for Naval Warfare Studies, U.S. Naval War College, Newport, RI), interview by the author, 15 April 2010.

[48] Ibid.

[49] Van Creveld, *Command in War*, 270-271.

[50] Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College), VIII-8.

[51] Gary Luck and Mike Findlay, *Insights & Best Practices: JTF level Command Relationships & Joint Force Organization, Focus Paper #4* (Suffolk, VA: Joint Warfighting Center, 2008), 12.

[52] Richard R. Burgess, "Connecting Commanders: Navy implements network of Maritime Operations Centers in fleet," *Seapower* (May 2009), 54-58.

[53] JP 3-0, *Joint Operations*, II-12.

[54] Vincent Alcazar, e-mail to the author, 29 April 2010. Lt Col Alcazar, USAF is an action officer for the Air-Sea Battle Concept on the Air Force staff. For background information on the Air-Sea Battle Concept, see Krepinevich, *Why AirSea Battle?*, 1-3.

[55] Mattis to U.S. Joint Forces Command, *C2 Vision*, memorandum.

Bibliography

Alberts, David S., and Hayes, Richard E. *Understanding Command and Control*. Washington, DC: CCRP Publication Series, 2006.

Amir Mizroch, Yaakov Katz. "Sailor Killed, Three Missing as Hizbullah Helped by Iran Fires Missile at Israeli Ship." *Jerusalem Post*, 16 July 2006, 1.

Ben-David, Alon, and Scott, Richard. "Intelligence failure led to strike on Hanit," *Janes Navy International*, 1 September 2006, http://search.janes.com (accessed 15 April 2010).

Bjorkland, Raymond C. *The Dollars and Sense of Command and Control*. Washington, DC: National Defense University Press, 1995.

Burgess, Richard R. "Connecting Commanders: Navy implements network of Maritime Operations Centers in fleet." *Seapower* (May 2009): 54-58.

Erickson, Andrew S., and Yang, David G. "On the Verge of a Game Changer." *U.S. Naval Institute Proceedings* (May 2009): 26-32.

Erickson, Andrew S, Lyle J. Goldstein, and William S. Murray. "Chinese Mine Warfare: A PLA Navy 'Assassin's Mace' Capability." *China Maritime Studies*, no. 3. Newport, RI: Naval War College, 2009.

Gordon, Andrew. *The Rules of the Game: Jutland and British Naval Command*. Annapolis, MD: Naval Institute Press, 2000.

Gray, Colin S. *Schools for Strategy: Teaching Strategy for 21st Century Conflict.* Strategic Studies Institute: Carlisle, PA, 2009.

Hoffman, Frank G. "Hybrid Warfare and Challenges." *Joint Force Quarterly*, Issue 52 (1st Quarter 2009), 34-37.

Information Warfare Monitor, and Shadowserver Foundation. *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Joint Report. http://shadows-in-the-cloud.net (accessed 10 April 2010).

Krepinevich, Andrew F. *Why AirSea Battle?* Washington, DC: Center for Strategic and Budgetary Assessments, 2010.

Luck, Gary, and Findlay, Mike. *Insights & Best Practices: JTF level Command Relationships & Joint Force Organization, Focus Paper #4*. Suffolk, VA: Joint Warfighting Center, 2008.

------. *Joint Operations Insights & Best Practices, 2nd ed*. Suffolk, VA: Joint Warfighting Center, 2008.

Mackey, James. "Recent US and Chinese Antisatellite Activity." *Air and Space Power Journal* (October 2009): 82-93.

Mattis, GEN James N., Commander U.S. Joint Forces Command to U.S. Joint Forces Command. *Command and Control (C2) Vision*, memorandum, 7 May 2008.

Mattis, GEN James N., Commander U.S. Joint Forces Command to U.S. Joint Forces Command, *Vision for a Joint Approach to Operational Design*, memorandum, 6 October 2009.

Norretranders, Tor. *The User Illusion: Cutting Consciousness Down to Size*. New York: Penguin, 1998.

Phillips, Michael M. "Civilians in the Crosshairs Slow Troops." *Wall Street Journal*¸ 22 February 2010, 1.

U.S. Department of Defense. *Irregular Warfare Joint Operating Concept*. Washington, DC: Department of Defense, September 2007.

------. *The Military Power of the People's Republic of China 2009*. Annual Report to Congress. Washington, DC: Office of the Secretary of Defense, 2009.

U.S. Office of Chairman of the Joint Chiefs of Staff. *Joint Operations*. Final coordination with Ch1, 13 Feb 2008. Joint Publication (JP) 3-0. Washington, DC: CJCS, 17 December 2006.

------. *Joint Task Force Headquarters*. Final coordination. Joint Publication (JP) 3-33. Washington, DC: CJCS, 16 February 2007.

Van Creveld, Martin. *Command in War*. Cambridge, MA: Harvard University Press, 1985.

Vego, Milan, N. "Future Warfare at Sea: Decline of Decision-Making in Naval Operations?" *Naval Forces* (January 2009): 8-15.

------. *Joint Operational Warfare: Theory and Practice.* Newport, RI: Naval War College, 2009.

Wasserbly, Daniel. "USJFCOM explores network-free warfighting," *Janes International Defence Digest*, 9 June 2009, http://search.janes.com (accessed 15 April 2010).

Woodcock, William A. "The Joint Forces Air Command Problem: Is Network-Centric Warfare the Answer?" *Naval War College Review* (Winter 2003):124-138.